APPENDIX D

TELEWORK AGREEMENT
SELF CERTIFICATION SECURITY CHECKLIST AND RESPONSIBILITIES

The following are the rules and policy in which the employee agrees to operate government furnished AIS equipment .

Security Checklist

1. Access:

   Are measures in place to ensure unauthorized individuals, to include family members do not have access to the AIS equipment?
   a. Are workstations/laptops password protected? Yes ____ No ____
   b. Are all passwords protected from access by unauthorized individuals? Yes ____ No ____
   c. Do all passwords adhere to the minimum length & format (8 characters, with a combination of letters, numbers and other characters (i.e. #, %, *)? Yes ____ No ____

2. Controls:

   a. Is all removable media handled and stored separately from personal media? Yes ____ No ____

   b. Is all removable media kept in a secure location to prevent unauthorized access? Yes ____ No ____

3. Markings:

   Is the workstation and media properly labeled with the appropriate security classification? Yes ____ No ____

4. Data Integrity:

   a. Does the workstation/laptop have personal firewall software installed? Yes ____ No ____
   b. Does the workstation/laptop have IPSEC Client Software installed? Yes ____ No ____
   c. Does the workstation/laptop have updated Norton & McAfee anti-virus software installed? Yes ____ No____

Initials _____

Security Responsibilities

1. As an employee of the Federal Government, or contractor employee to the government, and user of government automated information systems (AIS), computer equipment and software, you are responsible for understanding and complying with the provisions of AR 380-19 and AMC Supplement 1 to AR 380-19. This memorandum is directive in nature but not all-inclusive. Upon signing, this memorandum will be maintained by the appropriate Information Assurance Security Officer (IASO) and is subject to inspection. Specific responsibilities include:

a. Use government computer hardware and software only for its intended official purposes (see exceptions, para 2).

b. Protect data/information on your AIS as appropriate based on its classification or sensitivity level.

c. Protect your passwords for unclassified systems at a minimum of "For Official Use Only". Do not share your passwords with others.

d. Know your Information Assurance Security Officer (IASO), and Information Assurance Manager (IAM). (See the PEO, GCS Web-Site).

e. Report all computer security incidents and violations to your IASO, and the Information Assurance Manager (IAM) in SFAE-GCS-S, immediately.

f. Keep food and beverages away from AIS equipment.

g. Do not allow unauthorized personnel access to your AIS.

h. Do not use personally owned AIS equipment, software or games on the government work site or on government equipment (AIS) without prior written approval from your IASO.

i. Do not duplicate copyrighted software for personal use or allow others to copy the software you are using on your assigned government AIS. Copyright infringement is a serious crime. You must have a license for all software on the assigned AIS equipment.

j. Use all protective measures for each system and remember that all government owned and/or operated systems are subject to communications monitoring.

Initials _____

k. Only operate AIS equipment that has been accredited to process at the designated level of classification or sensitivity (i.e., Unclassified or Sensitive But Unclassified (SBU)). Teleworkers can not access or use information above SBU.

l. Report all stolen or missing software, hardware, or any AIS equipment to your supervisor, IASO, Security Coordinator, and the PEO, GCS IAM at SFAE-GCS-S.

m. Do not process **CLASSIFIED** information.

n. Mark all unclassified and media (floppy diskettes, zip disks, CD-ROMs) with the appropriate Standard Form (SF Label 710 for UNCLASSIFIED, or use a standard disk label and mark with the classification level, organization and date.

o. Use AMC Labels to mark the highest level of classification or sensitivity your AIS is accredited to process. Label your monitor, CPU, printer and scanner.

p. Do not send e-mail containing SBU information unless it has been encrypted. Do not forward your government e-mail to a commercial Internet Service Provider (ISP).

q. Access the Internet and the World Wide Web (WWW) only to support official mission requirements (see exceptions, para 2).

r. Remember that all communication on the Internet is open and unsecure. Only send unclassified public domain information over the Internet; never send SBU or classified information.

s. Do not send or forward erroneous, fictitious or other inappropriate messages, (virus hoaxes, chain letters, offensive e-mail).

t. Do not use the government equipment to publicize commercial products for personal gain.

u. Ensure all removable media is purged prior to turn-in.

2. EXCEPTIONS (with supervisor and IASO approval).

a. During duty hours, government communication resources (telephones, e-mail and the Internet) may be used for brief communications related to personal affairs. As a rule, brief means three minutes or less. This includes banking transactions, checking in with family, and making appointments. Whenever possible, communications should be made during non-duty hours, authorized breaks or lunch.

Initials _____

b. During non-duty hours, government communication resources may be used for longer periods for personal communications, professional development, training or browsing.

c. Above exceptions are subject to the following prohibitions:

(1) Use cannot result in any additional charges to the Government.

(2) Resources cannot be used for any activity that would bring discredit on the Army. Use good judgement. Bad judgement includes use involving pornography, racism, sexism and hate groups.

(3) Resources cannot be used for group mailings, profit or nonprofit business, political purposes or fundraising.

(4) The Internet may not be used without a current virus checker on the workstation. No system software may be downloaded and installed on the workstation without system administrator and IASO or IAM approval.

3. I CERTIFY THAT I HAVE READ AND UNDERSTAND THE ABOVE PROVISIONS.

_____	_____	_____	_____
NAME	SIGNATURE	ORGANIZATION	DATE

Initials _____